Aaditya Chomal, 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Decentralized Storage System: A Novel Approach to Secure and Resilient Data Management

Aaditya Chomal, Snehil Gamit, Sidharth Panda, Aqsa Rangrez, Govind, Yassir Farooqui
Faculty of Engineering and Technology Parul University
Vadodara, Gujarat, India

Abstract- In the modern digital landscape, traditional cen- tralized storage models are increasingly vulnerable to security breaches, suffer from single points of failure, incur high main- tenance costs, and present scalability limitations. The Decen- tralized Storage System (DSS) is proposed as an alternative solution, utilizing distributed ledger technologies, peer-to-peer (P2P) networks, and advanced cryptographic mechanisms to establish a fault-tolerant, secure, and highly available data storage infrastructure. This paper presents the design and implementation of a decentralized storage framework that integrates key blockchain concepts—such as immutability, transparency, and consensus validation—to enhance data integrity and security. The system enables users to store, retrieve, and share data in a fully decentralized manner while ensuring confidentiality through encryption. The work includes a comprehensive architectural and functional analysis of a full-stack, decentralized file storage platform built specifically on the Filecoin Protocol, leveraging the InterPlanetary File System (IPFS) for distributed content addressing and efficient data retrieval. The platform employs a hybrid architecture combining Web2 technologies—Next.js for the frontend, Node.js/Express for the backend, and MongoDB for centralized metadata management—with core Web3 protocols. The analysis confirms the project's success in creating a practical, non-custodial storage solution that abstracts the complexities of the decentralized web. However, a key architectural trade-off is identified: the system's reliance on provider-centric tooling (Boost CLI) and third-party Remote Procedure Call (RPC) endpoints (Glif API) simplifies development but introduces dependencies that compromise the ideal of full, end-to-end decentralization.

Keywords: Decentralized Storage, IPFS, Filecoin, Solana, Blockchain, DApp, Next.js, Express.js.

I. INTRODUCTION

The traditional digital landscape is dominated by centralized data storage, where a single entity, such as a cloud provider, controls the data's location, security, and accessibility. This architecture, while convenient, introduces a range of critical risks, including the potential for data loss due to server failure, unauthorized data access, and censorship by a controlling authority. Blockchain technology offers a paradigm shift by enabling the creation of decentralized applications (DApps) that operate on distributed networks, thus eliminating the need for a central intermediary.

This paper documents the architecture and implementation of a DApp that serves as a decentralized storage system. The project's core objective is to provide a more secure and re- silient alternative to traditional storage solutions by combining a user-friendly web interface with the verifiable, peer-to-peer nature of decentralized networks. The system achieves this by integrating a high-performance blockchain for identity and authentication with a two-part decentralized storage protocol that separates data distribution from long-term persistence. The result is a proof-of-concept that establishes a secure, transparent, and censorship-resistant method for managing digital assets.

II. LITERATURE REVIEW

Traditional centralized cloud storage systems such as Ama- zon Web Services (AWS) and Google Cloud suffer from critical issues including single points of failure, data breaches, and lack of user control over data. To address these limita- tions, decentralized storage systems (DSS) leverage blockchain technology, peer-to-peer (P2P) networking, and cryptographic hashing to enhance data security, integrity, and availability.

The InterPlanetary File System (IPFS) introduces content- based addressing, allowing files to be identified by crypto- graphic hashes instead of physical locations, thus eliminating reliance on centralized servers. However, IPFS lacks a built- in incentive mechanism for data persistence. To overcome this, Filecoin integrates an economic layer that incentivizes data storage using blockchain-based proofs such as Proof-of- Replication (PoRep) and Proof-of-Spacetime (PoSt) to ensure verifiable and continuous data availability.

Comparative analyses reveal that Filecoin, Arweave, Storj, and Sia address different aspects of decentralized storage. Filecoin focuses on scalable and temporary storage through a market-driven model, Arweave ensures permanent archival storage via a one-time payment mechanism, while Storj and Sia provide decentralized cloud storage with enhanced redun- dancy and encryption.

The reviewed system employs a hybrid full-stack architec- ture, integrating Web2 frameworks (Next.js, Node.js, Mon- goDB) with Web3 technologies (IPFS, Filecoin) to provide a secure and user-friendly decentralized storage platform. The use of non-custodial wallet-based authentication enhances security, though reliance on centralized metadata and third- party RPC endpoints introduces minor centralization concerns. Future research directions suggest implementing smart con- tracts for automated deal management, supporting multi-provider interoperability, and optimizing deal batching mech- anisms for large-scale deployment. Collectively, decentralized storage systems signify a pivotal advancement toward a secure, transparent, and user-controlled digital ecosystem.

III. EXISTING DECENTRALIZED STORAGE PLATFORMS

Several decentralized storage platforms have emerged to provide secure, efficient, and censorship-resistant alternatives to traditional cloud storage. IPFS (InterPlanetary File System) is a peer-to-peer protocol that enables users to store and share files using content-based addressing, ensuring data integrity and reducing duplication. Filecoin, built on top of IPFS, introduces a blockchain-based incentive layer where users earn tokens for renting out unused storage space. Storj utilizes encryption and file sharding to distribute data across multiple nodes, improving security and reliability while maintaining user privacy. Sia also leverages blockchain technology to create smart contracts between users and hosts, ensuring transparent and verifiable storage deals. Meanwhile, Arweave focuses on permanent data storage through its "blockweave" structure, ideal for archival and immutable data. These plat- forms collectively demonstrate the potential of decentralized networks to overcome limitations of centralized systems, such as data breaches, single points of failure, and lack of user control.

IV. ANALYSIS OF EXISTING DECENTRALIZED STORAGE SYSTEMS

Decentralized storage systems aim to overcome the lim- itations of traditional centralized cloud storage by offering improved data privacy, integrity, and availability through dis- tributed architectures. Several leading platforms have emerged, each implementing unique mechanisms for data distribution, encryption, and incentivization.

A. IPFS (InterPlanetary File System)

IPFS uses a peer-to-peer network with content-addressed storage, where files are identified by cryptographic hashes. This approach ensures data integrity and deduplication. How- ever, IPFS alone does not guarantee data persistence—content remains available only while at least one node pins it.

B. Filecoin

Built on IPFS, Filecoin introduces a blockchain-based incen- tive layer. It employs Proof-of-Replication (PoRep) and Proof- of-Spacetime (PoSt) to verify that storage providers retain client data over time. Filecoin enables an open marketplace for buying and selling storage but faces complexity due to blockchain transaction overheads.

C. Storj

Storj emphasizes client-side encryption and data shard- ing. Files are encrypted, split into multiple fragments, and distributed across independent nodes, ensuring both privacy and redundancy. While it provides strong performance, its partially centralized components (called satellites) can limit full decentralization.

D. Sia

Sia leverages smart contracts between renters and hosts to facilitate storage agreements. Data is encrypted, fragmented, and replicated across hosts, providing transparency and verifi- ability. However, the network's smaller host base may impact overall availability compared to larger ecosystems.

E. Arweave

Arweave introduces a "blockweave" architecture to achieve permanent data storage. Its economic model ensures a one- time payment for indefinite data retention, making it ideal for archival purposes. Nevertheless, permanent storage raises challenges related to legal compliance and scalability.

F. Comparative Analysis

Table I summarizes key characteristics of major decen- tralized storage systems. Each platform balances trade-offs among decentralization, performance, and usability. IPFS and Filecoin focus on integrity and incentives, while Storj and Sia emphasize privacy and cost-efficiency. Arweave, in contrast, targets immutability and permanence.

TABLE I

Feature	IPFS	Filecoin	Storj	Sia
Content Addressing	Yes	Yes	Yes	Yes
Incentive Layer	No	Yes	Partial	Yes
Client Encryption	Optional	Optional	Yes	Yes
Permanent Storage	No	Deal-based	Lease-based	Deal-based
Decentralization	High	High	Medium	High
Best Use Case	CDN, Web3	Archival	Secure Backup	Low-cost Storage

V. FINDINGS AND DISCUSSION

The analysis of existing decentralized storage platforms reveals that while substantial progress has been made in distributed data management, several technical and economic limitations still hinder large-scale adoption.

A. **Key Findings**

1) **Incentive Mechanisms:** Platforms such as Filecoin and Sia successfully integrate blockchain-based incentives to ensure long-term storage reliability. However, the high computational and transactional costs associated with on-chain proofs remain a barrier to scalability.

2) **Data Privacy and Security:** Systems like Storj and Sia prioritize user privacy through client-side encryption and data fragmentation. This minimizes the risk of unauthorized access, though it introduces challenges in efficient retrieval and repair operations.

3) Permanence and Immutability: Arweave's design en- sures permanent storage, which is advantageous for archiving immutable records. Yet, the irreversibility of stored data conflicts with modern data regulations such as GDPR's right to erasure.

4) Performance and Accessibility: IPFS provides efficient content distribution through peer-to-peer file sharing, but availability heavily depends on network nodes main- taining pinned content. Systems relying solely on peer availability often face higher retrieval latency.

5) Decentralization vs. Usability: Fully decentralized sys- tems maintain greater resilience and censorship resis- tance but often suffer from lower usability and slower performance. Hybrid models, such as Storj's partially centralized coordination nodes, improve efficiency at the expense of full decentralization.

B. Performance Trade-offs

Decentralized storage systems must balance three com- peting objectives: security, availability, and cost-eflciency. Systems emphasizing redundancy and encryption incur higher storage overheads, while those focusing on cost efficiency may compromise fault tolerance. Filecoin's robust economic incentives, for instance, improve reliability but lead to higher operational complexity. Conversely, IPFS achieves simplicity and flexibility but lacks a built-in persistence guarantee.

C. Research Gaps and Future Directions

Despite their advancements, current decentralized storage solutions still face open research challenges: label=3)

- **Scalable Verification:** Designing lightweight, off-chain proof mechanisms to verify storage integrity without increasing blockchain load.
- **Hybrid Persistence Models:** Combining economic in- centives with curated pinning networks to ensure long- term data availability.
- **Privacy-Preserving Retrieval:** Developing protocols for secure and anonymous content retrieval using zero- knowledge proofs or private information retrieval (PIR) techniques.
- **Interoperability and Standardization:** Establishing common APIs and data standards to enable seamless in- teraction across different decentralized storage networks.
- **Legal and Ethical Compliance:** Introducing selective mutability or content expiration mechanisms that main- tain decentralization while complying with international data protection laws.

VI. PROPOSED SYSTEM

The proposed Decentralized Storage System (DSS) intro- duces a novel approach to distributed data storage by inte- grating conventional web development technologies with de- centralized blockchain protocols. Unlike existing decentralized storage solutions that primarily focus on blockchain-centric mechanisms, the DSS employs a hybrid full-stack architecture combining Next.js, Node.js, and MongoDB for Web2 function- ality with IPFS and Filecoin for Web3-based data storage and validation. This integration enables a seamless bridge between user-friendly web interfaces and decentralized data operations. The system differentiates itself from existing platforms such as Arweave, Storj, and Sia by offering a scalable, cost- effective, and developer-accessible framework that simplifies interaction with decentralized infrastructure. Through features such as non-custodial wallet-based authentication, automated deal management, and real-time Filecoin deal tracking, the DSS enhances both user autonomy and operational efficiency. Moreover, the inclusion of Boost CLI for backend automation and MongoDB for fast metadata indexing provides a balanced trade-off between decentralization and performance. This hy- brid and user-centric approach positions the DSS as a practical model for the next generation of decentralized storage systems, combining transparency, security, and usability.

VII. SYSTEM ARCHITECTURE

The application is structured as a full-stack DApp with a clear separation of concerns across three distinct layers: the frontend, the backend, and the blockchain with its associated decentralized storage network. This architecture is designed to balance the benefits of decentralization with the performance and scalability requirements of a modern web application.

- Frontend Layer

The user interface is a web application built using the Next.js framework, which is a React framework that supports server and client data fetching and can be used to build API endpoints to securely connect with third-party services. It is responsible for client-side rendering and user interaction, providing the visual and functional components that allow the user to interact with the decentralized network.

- **Backend Layer**

The server-side logic is managed by a Node.js server utilizing the Express.js framework. This backend serves two primary purposes: API management and file processing. It handles requests from the frontend, including user authenti- cation and file uploads. For file uploads, the backend uses Multer, a Node.js middleware specifically designed to handle multipart/form-data, which is the standard format for file uploads.

- **Blockchain and Decentralized Storage Layer**

This layer is the core of the system and combines several powerful, decentralized technologies.

- **Blockchain:** The project uses the Solana blockchain, which is known for its ability to host scalable DApps and for its high transaction speed and low fees compared to rival blockchains like Ethereum.
- **User Authentication:** Instead of traditional passwords, the DApp authenticates users via their blockchain wallet. The user connects their Phantom Wallet, a popular self- custodial wallet for the Solana ecosystem. To log in, the user signs a message with their private key, creating a digital signature that acts as a digital fingerprint to prove ownership and authorization. The backend then verifies this signature to prove the user's ownership and authorization, after which it can issue a session token (e.g., JWT) to manage the user's authenticated state on the platform.
- **Decentralized Storage Protocol:** The system uses a two- part approach to decentralized storage, combining IPFS and Filecoin. IPFS is a peer-to-peer network that stores and distributes files based on their content, with each file given a unique identifier (CID). However, IPFS storage is not permanent on its own and relies on "pinning" to persist data. This is where Filecoin, a decentralized storage network built on top of the IPFS protocol, comes in. Filecoin provides a market-based approach where users can pay with FIL tokens to storage providers to host their data, thus ensuring long-term data availability. Storage providers use a tool like the Filecoin Boost CLI to manage data storage and retrieval on the network.
- **File Conversion and Metadata:** The backend converts uploaded files into a Content Addressable aRchive (CAR) file, a format used by IPFS to store and trans- fer data. This is done using a command-line tool like go-car. Once the file is converted and pinned, essential metadata—including the file's unique CID, the user's ID, and the file's path—is stored in a traditional database like MongoDB for quick access and management.

VIII. METHODOLOGY

The user's interaction with the decentralized storage system follows a clear, secure, and end-to-end process:

- **User Login:** The user visits the Next.js frontend and connects their Phantom Wallet. The application requests that the user sign a message, which is then sent to the Express.js backend for signature verification.
- **Authentication:** The backend verifies the signature, prov- ing the user's identity, and issues a JWT to establish a secure, authenticated session.
- **File Upload:** The user selects and uploads a file through the Next.js interface. The Express.js backend receives the file using the Multer middleware.
- **File Conversion:** The backend processes the raw file and converts it into a CAR file using the go-car tool.
- **IPFS and Filecoin Storage:** The CAR file is then pinned to the IPFS network. Simultaneously, the backend initiates

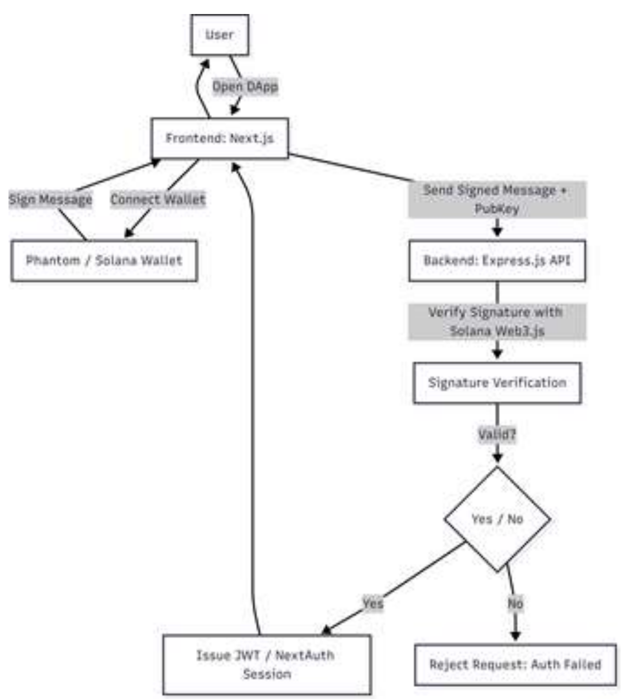

Fig. 1. User Authentication Flow with Solana and Phantom Wallet.

a storage deal on the Filecoin network using the Filecoin Boost CLI, which ensures the data's long-term persistence through an incentivized market.

- **Metadata Storage:** The unique CID and other relevant file information are saved to the MongoDB database, linking the file to the user's account for easy retrieval. The backend then responds to the frontend with a success message, and the frontend updates the user interface to show the newly uploaded file.

IX. RESULT

This project successfully demonstrates a viable model for a decentralized storage system. By leveraging the combined strengths of a Next.js/Express.js web application and the Solana/IPFS/Filecoin network, the platform provides a robust alternative to centralized storage. The separation of concerns between the fast, low-cost Solana blockchain for authentication and the permanent, verifiable storage of Filecoin creates a highly efficient and trustworthy system.

The primary benefits realized by this model are enhanced security, improved data integrity, and increased censorship resistance. Since data is stored across a peer-to-peer network rather than on a single server, it is more resilient and resistant to attack. Furthermore, the use of content-addressed CIDs ensures that files are tamper-proof.

Future work could focus on enhancing the long-term data management aspects of the platform. A key area for improve- ment is to integrate the system with academic data repositories, such as Figshare or Harvard Dataverse [1, 2], which can assign persistent Digital Object Identifiers (DOIs) to uploaded datasets.[3, 2] This would make the research data permanently citable and discoverable by other researchers, further promoting open and transparent research practices.

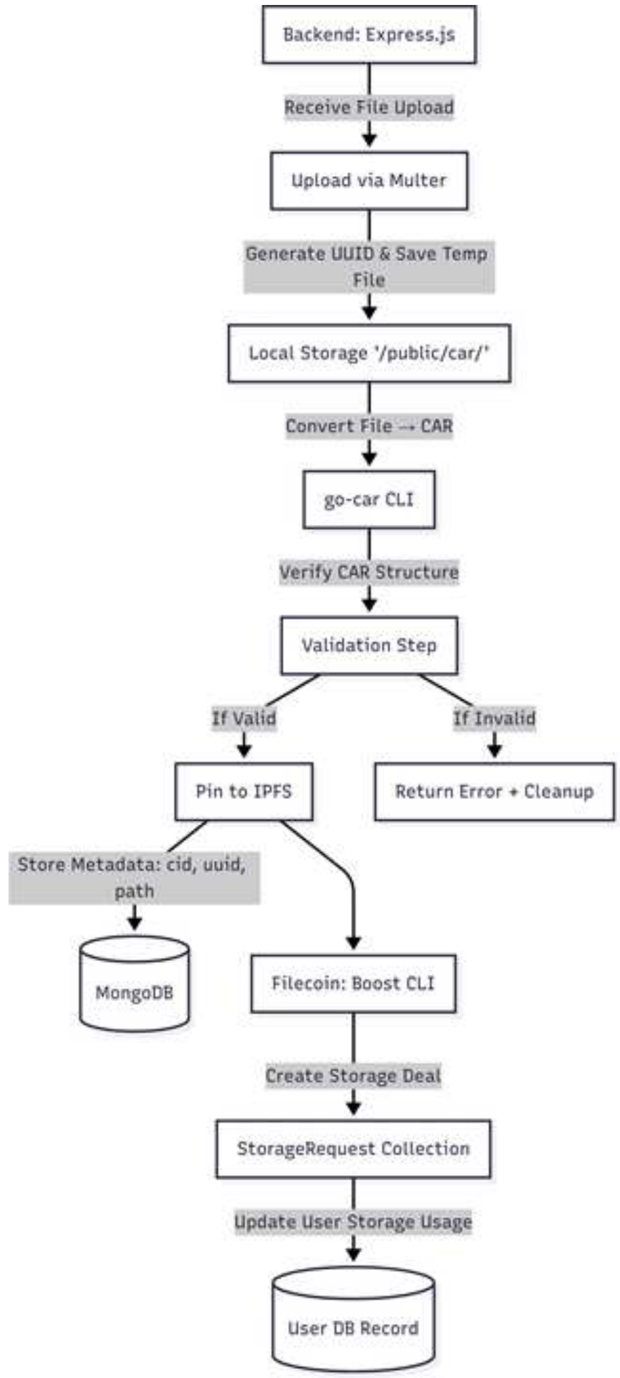

Fig. 2. File Upload and Decentralized Storage Workflow.

A. System Workflow Verification

The user's interaction with the decentralized storage system follows a clear, secure, and end-to-end process,the platform was verified to function correctly across all key workflows:

- **User Login and Wallet Integration:** :The user visits the Next.js frontend and connects their Phantom or Solana Wallet. The application requests that the user sign a message, which is then sent to the Express.js backend for signature verification.

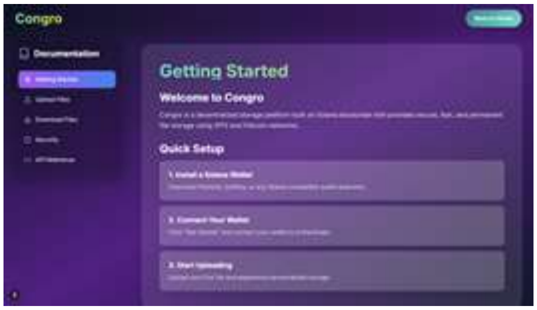

Fig. 3. Login page with integrated Solana wallet connectivity.

2) User Dashboard: :Regular users access a personalized dashboard displaying their active policies and a submission form for new claims, as shown in Fig. 4. This ensures that users interact only with data relevant to their account.

Fig. 4. User Dashboard showcasing storage usage.

3) File Transaction: :Direct blockchain interaction is a core feature of the DApp. Th Fig.5 shows the transaction done.

Fig. 5. Confirmation of File transaction.

X. CONCLUSION AND FUTURE WORK

A. Conclusion

The proposed Decentralized Storage System (DSS) effec- tively addresses the limitations of centralized storage by uti- lizing blockchain, peer-to-peer networking, and cryptographic mechanisms to ensure secure, transparent, and reliable data management. Through its hybrid Web2–Web3 architecture, integrating Next.js, Node.js, MongoDB, IPFS, and Filecoin, the system provides a scalable and user-friendly framework for decentralized storage. Features such as non-custodial authen- tication, automated deal initiation, and metadata management simplify complex decentralized processes while maintaining user control and data integrity. Compared to existing platforms like Arweave, Storj, and Sia, the DSS offers improved accessi- bility and scalability. Future work will focus on incorporating smart contracts and multi-provider integration to achieve full decentralization and enhanced efficiency.

B. Future Work

The proposed Decentralized Storage System (DSS) can be further enhanced through the following developments:

- **Smart Contract Integration:** • Deploy smart contracts on the Filecoin Virtual Machine (FVM) to automate payments, deal initiation, and renewals.
- **Multi-Provider Storage Support:** • Integrate with other decentralized platforms such as Arweave, Storj, and Sia to provide flexible and cost-efficient data storage options.
- **Event-Driven Deal Tracking:** • Replace periodic polling with real-time, event-based tracking for improved system re- sponsiveness and efficiency.
- **Optimized Data Batching**: • Implement batch processing for multiple file uploads and large datasets to reduce transaction overhead.
- **Decentralized Metadata Management:** • Shift from central- ized MongoDB storage to distributed databases or IPFS-based metadata storage to eliminate single points of failure.
- **Enhanced Security and Privacy:** • Employ stronger encryp- tion and fine-grained access

control to protect data integrity and user confidentiality.

- **Scalability Improvements:** • Optimize system performance and network load balancing to support higher throughput and large-scale adoption.

REFERENCES

1. P. Alisha Lobo and V. Sarasvathi, "Distributed File System of Medical Data Using Interplanetary File System and Blockchain Technology," in Proc. Int. Conf. Computer Science and Engineering (ICSE), PES University, Bangalore, India, pp. 1–5, IEEE, 2024.
2. B. Han, Z. Liang, Y. Huang, M. Qin, and F. Xiong, "Research on Collaborative Storage of Data Based on IPFS and Blockchain," in Proc. Int. Conf. Big Data and Intelligent Engineering, Southwest Forestry University, Kunming, China, pp. 1–6, IEEE, 2024.
3. R. A. Nayak, N. Prakash, N. S., and N. V., "Decentralized File Storage Platform Using IPFS and Blockchain," in Proc. Int. Conf. Information Science and Engineering (ICISE), B. M. S. College of Engineering, Bangalore, India, pp. 1–5, IEEE, 2024.
4. J. Mahajan and A. Prachi, "Decentralized File Storage: Leveraging Blockchain, Polygon, Web3, and IPFS," in Proc. Int. Conf. Emerging Technologies in Computer Science and Engineering (ETCSE), Parul University, Vadodara, India, pp. 1–5, IEEE, 2024.
5. M. P. K, S. Chandrappa, K. B. V. Brahma Rao, B. H. K, Y. Farooqui, and Y. Dharangutti, "Blockchain-based Secure Communication Model for Protecting Sensor Network Data Integrity in Smart Agriculture Systems," in 2025 3rd Int. Conf. Data Science and Information System (ICDSIS), Hassan, India, 2025, pp. 1–5, doi: 10.1109/ICDSIS65355.2025.11071174.
6. K. Sivasankari and V. S. Sathyamithran, "IPFS Enabled Robust Mecha- nism for File Storage and Retrieval Using Blockchain," in Proc. Int. Conf. Computer Science and Information Technology (ICCSIT), SRM Institute of Science and Technology, Chennai, India, pp. 1–5, IEEE, 2022.
7. P. Kumar, M. Gupta, and R. Kumar, "Improved Cloud Storage System Using IPFS for Decentralised Data Storage," in Proc. Int. Conf. Cloud Computing and Decentralized Systems (ICCCDS), Chandigarh Univer- sity, Punjab, India, pp. 1–5, IEEE, 2024.
8. S. Agal, K. M. Raulji, Y. Farooqui, N. Bhavsar, and R. Agrawal, "Innovative Financial Services Driven by AI and Blockchain Syn- ergy for Decentralized Trust and Personalized Solutions," in 2024 IEEE 2nd Int. Conf. Innovations in High Speed Communication and Signal Processing (IHCSP), Bhopal, India, 2024, pp. 1–8, doi: 10.1109/IHCSP63227.2024.10959960.
9. J. Anthal, S. Choudhary, and R. Shettiyar, "Decentralizing File Sharing: The Potential of Blockchain and IPFS," in Proc. Int. Conf. Decentralized Systems and Emerging Technologies (ICDSET), Thakur College of Science and Commerce, Mumbai, India, pp. 1–6, IEEE, 2023.
10. I. B. Prakash, A. K. Tiwari, and U. Hariharan, "Decentralized Metadata Storage for Non-Fungible Token Collections Using Interplanetary File System," in Proc. Int. Conf. Blockchain and Decentralized Applications (ICBDA), Apex Institute of Technology, Chandigarh University, Mohali, Punjab, India, pp. 1–6, IEEE, 2023.
11. H. Amin, M. K. Chahine, and G. Mazzini, "P2P Application for File Sharing," in Proc. Int. Conf. Peer-to-Peer Systems (ICP2PS), University of Damascus, Syria, and University of Ferrara, Italy, pp. 1–5, IEEE, 2012.
12. Y. Farooqui, D. Patel, M. Kumar, R. Mehta, and R. Vyas, "Towards a Decentralized Future: The Role of DeVerse in Publishing Evolution," in 2024 Parul Int. Conf. Engineering and Technology (PICET), Vadodara, India, 2024, pp. 1–6, doi: 10.1109/PICET60765.2024.10716144.
13. S. B. Prasad, A. K. A. R., and R. V. Honnungar, "Blockchain-Based Scal- ability Solutions for IoT: A Decentralized Design to Enhance Performance and Security," in Proc. Int. Conf. Internet of Things and Decentralized Systems (ICIoTDS), RV College of Engineering and RNS Institute of Technology, India, pp. 1–6, IEEE, 2024.
14. R. Li, J. Hai, and F. Wan, "Decentralized Data Subscription System: A Multi-Chain Blockchain

and IPFS Integration," in Proc. 4th Int. Conf. Computer Science and Blockchain (CCSB), Zhengzhou University and State Grid Xuchang Power Supply Company, China, pp. 1–6, IEEE, 2024.

15. J. Xiong, Y. Hu, G. Li, R. Tang, and Z. Fan, "Metadata Distribution and Consistency Techniques for Large-Scale Cluster File Systems," in Proc. Int. Conf. Distributed and Cluster File Systems (DCFS), pp. 1–7, IEEE, 2011.
16. R. Nygaard, H. Meling, and J. I. Olsen, "Cost-effective Data Upkeep in Decentralized Storage Systems," in Proc. 38th ACM/SIGAPP Symposium on Applied Computing (SAC '23), Tallinn, Estonia, Mar. 27–31, 2023, Article 4, 9 pages, ACM, 2023.
17. Y. Zhu, C. Lv, Z. Zeng, J. Wang, and B. Pei, "Blockchain-based Decentralized Storage Scheme," in Proc. Int. Conf. Information and Electrical Engineering (ICIEE), China Agriculture University and Third Research Institute of Ministry of Public Security, China, pp. 1–6, IEEE, 2023.
18. Y. Farooqui and S. M. Parikh, "Secure and Transparent Supply Chain Management Using Blockchain and IoT," Int. J. Recent Innovation Trends, 2023.
19. P. B. Patil, A. R. Hujare, K. S. Desai, V. B. Devkar, and H. I. Bhadgaonkar, "Decentralized File Storage System Using Blockchain," in Proc. Int. Conf. Artificial Intelligence and Data Science (ICAIDS), Sharad Institute of Technology College of Engineering, Yadrav, India, pp. 1–6, IEEE, 2023.
20. A. Rathour, A. Shahi, A. Tiwari, and B. Maurya, "Review Paper on Decentralized File System (Storage and Sharing) Using Blockchain," in Proc. Int. Conf. Emerging Technologies in Information Technology (ICETIT), Institute of Technology and Management, Gorakhpur, Uttar Pradesh, India, pp. 1–5, IEEE, 2023.
21. N. Gajare, A. Raotole, P. Shetty, A. Lodha, and J. S. Mahajan, "Survey Paper on Decentralised Cloud Storage Using IPFS," Int. Res. J. Modernization Eng. Technol. Sci. (IRJMETS), vol. 6, no. 2, Feb. 2024, pp. 1–6, doi: 10.56726/IRJMETS49167.
22. J. Wang, W. Ou, W. Wang, R. S. Sherratt, Y. Ren, and X. Yu, "Data Security Storage Mechanism Based on Blockchain Network," Computers, Materials & Continua, vol. 74, no. 3, pp. 4933–4950, 2023.
23. "MedRSS: A Blockchain-based Scheme for Secure Storage and Sharing of Medical Records," Computers & Industrial Engineering, vol. 183, Article 109521, Sept. 2023.
24. S. Jain, N. Marriwala, P. Singh, C. C. Tripathi, and D. Kumar, "Storage and Organisation of Geospatial Data in Distributed Blockchain Using IPFS," in Emergent Converging Technologies and Biomedical Systems (ETBS), Lecture Notes in Electrical Engineering, vol. 1116, Springer, Singapore, 2024, pp. 583–596.
25. M. Xu, J. Zhang, H. Guo, X. Cheng, D. Yu, Q. Hu, Y. Li, and Y. Wu, "FileDES: A Secure, Scalable and Succinct Decentralized Encrypted Storage Network," Cryptology ePrint Archive, Paper 2024/182, 2024.
26. B. Zhou, J. Zhao, G. Chen, and Y. Yin, "Research on Secure Storage Technology of Spatiotemporal Big Data Based on Blockchain," Applied Sciences, vol. 13, no. 13, Article 7911, 2023.
27. "The Key Security Management Scheme of Cloud Storage Based on Blockchain and Digital Twins," Journal of Cloud Computing, vol. 13, Article 15, 2024.
28. S. Li, T. Zhou, H. Yang, and P. Wang, "Blockchain-Based Secure Storage and Access Control Scheme for Supply Chain Ecological Business Data: A Case Study of the Automotive Industry," Sensors, vol. 23, no. 16, Article 7036, 2023.
29. H. Tian and G. Huang, "Research on Distributed Secure Storage Framework of Industrial Internet of Things Data Based on Blockchain," Electronics, vol. 13, no. 23, Article 4812, 2024.
30. M. B. Saif, S. Migliorini, and F. Spoto, "Efficient and Secure Dis- tributed Data Storage and Retrieval Using Interplanetary File System and Blockchain," Future Internet, vol. 16, no. 3, Article 98, 2024.
31. E. Daniel and F. Tschorsch, "IPFS and Friends: A Qualitative Compar- ison of Next Generation Peer-to-Peer Data Networks," arXiv preprint arXiv:2102.12737, 2022.